DATE(S) ISSUED:
10/12/2010

SUBJECT:
Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-071)

OVERVIEW:
Ten vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
        Internet Explorer 6
        Internet Explorer 7
        Internet Explorer 8
        Windows XP
        Windows Server 2003
        Windows Server 2008
        Windows Vista
        Windows 7

RISK:
Government:
        Large and medium government entities: **High**
        Small government entities: **High**

Businesses:
        Large and medium business entities: **High**
        Small business entities: **High**

Home users: High

DESCRIPTION:
Ten vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

AutoComplete Information Disclosure Vulnerability
An information disclosure vulnerability exists in Microsoft Internet Explorer that could allow a remote attacker access to sensitive data. More specifically, a vulnerability exists that could potentially allow form data within Internet Explorer to be captured via the AutoComplete feature. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker viewing information previously entered into input fields after the AutoComplete feature has been enabled.

Two HTML Sanitization Vulnerabilities

Two information disclosure vulnerabilities exist in Microsoft Internet Explorer that could allow a remote attacker access to sensitive data. More specifically, two vulnerabilities exist in the way that the 'toStaticHTML' API sanitizes HTML that could allow an attacker to perform cross-site scripting attacks and run scripts in the security context of the logged-on user. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker executing scripts in the victim's security context.

CSS Special Character Information Disclosure Vulnerability
An information disclosure vulnerability exists in Microsoft Internet Explorer that could allow a remote attacker access to sensitive data. More specifically, a vulnerability exists in the way that Internet Explorer processes CSS special characters. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker viewing content from another domain or Internet Explorer zone.

Four Uninitialized Memory Corruption Vulnerabilities
Four remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Anchor Element Information Disclosure Vulnerability
An information disclosure vulnerability exists in the way that Internet Explorer improperly handles the Anchor element. This behavior occurs during user operation when the Anchor element is not removed during content pasting and editing, potentially revealing personally identifiable information intended for deletion. While this is not an exploitable vulnerability, it can potentially expose previously deleted content during user operation.

Cross-Domain information Disclosure Vulnerability
An information disclosure vulnerability exists in Microsoft Internet Explorer that could allow a remote attacker access to sensitive data. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining access to another domain or Internet Explorer zone.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-071.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0808
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3243
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3324
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3325
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3326
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3327
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3328

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3329
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3330
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3331